National Infrastructure Protection Center
CyberNotes

Issue #2001-17 *August 27, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between August 9 and August 24, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
4D Incorporated[1]	Windows 98se/NT 4.0/2000	4D WebServer 6.5.7	A directory traversal vulnerability exists when an improperly constructed HTTP request is sent, which could let a remote malicious user view sensitive information.	No workaround or patch available at time of publishing.	4D WebServer Directory Traversal	Medium	Bug discussed in newsgroups and websites.
Adobe[2]	Unix	Acrobat Reader (UNIX) 4.05	A vulnerability exists because Acroread creates the AdobeFnt.lst file with default world-writable permissions, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AcroRead Insecure Default Font List Permissions	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Bugtraq, August 20, 2001.

[2] Securiteam, August 24, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Group[3]	Unix	Apache 1.3.14, 1.3.17, 1.3.19, 1.3.20	A remote Denial of Service vulnerability exists because it is possible to bypass mod_rewrite rules if the rules are constructed in a certain way.	Unofficial workaround (Bugtraq): Use of the following rule design is recommended: RewriteCond %{HTTP_REFERER} !^http://www\.yoursite\.com$ RewriteRule ^/*images/*.* - [G]	Apache Mod ReWrite Rules Bypassing Image Linking	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Group[4]	Unix	Tomcat 3.2.1	A vulnerability exists when an exception is thrown in a Java Server Page, which could let a malicious user gain sensitive information.	Unofficial workaround (Bugtraq): As a workaround, users can create custom error pages using the <error-page> directive in web.xml.	Tomcat Error Message Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
ASCII NT, Incorporated[5]	Windows 95/98/NT 4.0/2000	WinWrapper Professional 2.0	A directory traversal vulnerability exists due to insufficient validation of input, which could let a remote malicious user view sensitive information.	Update available at: http://www.tsc.ant.co.jp/products/download.htm	WinWrapper Admin Server Arbitrary File Reading	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
A-V Tronics[6]	Windows 98/NT 4.0/2000	InetServ 3.0, 3.1.1, 3.2.1	A buffer overflow vulnerability exists in the webmail interface, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	InetServ Webmail Authentication Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
BadBlue[7]	Windows 95/98/ME/ NT 4.0/2000	BadBlue Personal Edition 1.02 beta	An input validation vulnerability exists due to a lack of checks for NULL bytes, which could let a malicious user download the full source code of .PHP pages.	No workaround or patch available at time of publishing.	BadBlue Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Baltimore Technologies[8]	Windows NT 4.0	WEB sweeper 4.0, 4.02	Two vulnerabilities exist: a vulnerability that allows malicious users to execute arbitrary JavaScript by bypassing the filtering mechanism; and a vulnerability exists because scripting code from web pages is not properly filtered, which could let a malicious user execute scripting code of his choice.	No workaround or patch available at time of publishing.	WEBsweeper Unicode Script Filtering and Script Filtering Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the Script Filtering Bypass Vulnerability.

[3] Bugtraq, August 12, 2001.

[4] Bugtraq, August 16, 2001.

[5] Secure Net Service(SNS) Advisory No.39, August 20, 2001.

[6] Strumpf Noir Society Advisories, August 22, 2001.

[7] Securiteam, August 23, 2001.

[8] Securiteam, August 15, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cerberus[9]	Windows 95/98/NT 4.0/2000	FTP Server 1.5	A directory traversal vulnerability exists which could let a malicious user view sensitive information.	No workaround or patch available at time of publishing.	Cerberus FTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Dynu[10]	Windows 95/98/NT 4.0/2000	Dynu FTP Server 1.05 and prior	A directory traversal vulnerability exists which could let a malicious user view sensitive information.	Upgrade available at: http://www.dynu.com/dynuftpserver.asp	Dynu FTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites.
FreeBSD[11]	Unix	FreeBSD 3.5, 3.5-STABLE, 3.5.1-RELEASE & STABLE, 4.0, 4.1, 4.1.1-4.3 RELEASE & STABLE	A vulnerability exists when an unprivileged process is debugging a privileged one, which could let a malicious user view sensitive information.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT	FreeBSD linprocfs Privileged Process Memory Disclosure	Medium	Bug discussed in newsgroups and websites.
FreeBSD[12]	Unix	FreeBSD 4.3-RELEASE, 4.3-STABLE	A vulnerability exists when "IPFW" is used with the "me" identifier on a point to point interface, which potentially could let a remote malicious user compromise local resources.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:53/ipfw.patch	FreeBSD IPFW Me Point To Point Interface Address Addition	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
glFtpD [13]	Unix	glFtpD 1.13.6, 1.16.9. 1.17.2, 1.18a, 1.19, 1.20, 1.21, 1.22b, 1.23	A Denial of Service vulnerability exists whenever a specially formed "LIST" command is received.	Upgrade available at http://www.glftpd.org/glftpd.html	glFtpD LIST Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Intego[14]	MacOS 7.0-9.1	FileGuard 4.0	A vulnerability exists because passwords are stored unencyrpted, which could let a malicious user elevate his privileges.	No workaround or patch available at time of publishing.	Intego FileGuard Weak Password Encryption	Medium	Bug discussed in newsgroups and websites.
Knox Software[15]	Unix	Arkeia Server 4.2.8-2	Two password vulnerabilities exist which could let a malicious user gain access to the password file and log in as root.	No workaround or patch available at time of publishing.	Arkeia Server Static Salt Weak Password and Blank Default Root Password	**High**	Bug discussed in newsgroups and websites. No exploit code is required for the Blank Default Root Password vulnerability.

[9] Securiteam, August 21, 2001.
[10] Securiteam, August 22, 2001.
[11] FreeBSD Security Advisory, FreeBSD-SA-01:55, August 21, 2001.
[12] FreeBSD Security Advisory, FreeBSD-SA-01:53, August 17, 2001.
[13] Asguard Labs Advisory, August 17, 2001.
[14] Bugtraq, August 20, 2001.
[15] Bugtraq, August 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Lotus[16]	Windows NT 4.0/2000, OS/2 4.5Warp, OS/390 V2R9, Unix	Lotus Domino 4.6.1, 4.6.3, 4.6.4, 5.0.1-5.0.8	A Denial of Service vulnerability exists when a message is received by the server with the mail recipient set as being at a domain that is not local to the server and the sender as bounce@[127.0.0.1].	No workaround or patch available at time of publishing.	Lotus Domino Mail Loop Denial of Service	Low	Bug discussed in newsgroups and websites.
Microsoft[17]	Windows 2000	Internet Information Server 4.0 (IIS buffer overflow vulnera-bility), 5.0	Five vulnerabilities exist: a buffer overflow vulnerability exists involving the code that performs server-side include (SSI) directives, which could let a malicious user execute arbitrary code; a privilege elevation vulnerability exists due to a flaw in a table that IIS 5.0 uses, which could let a malicious user with write permission run any code with System privileges; and three Denial of Service vulnerabilities exist, one when the server is preparing the MIME headers for the response to a HTTP request for a certain type of file; one in the way malformed requests are handled by WebDAV; and one of which keeps IIS 5.0 from serving content until the admin removes the spurious entry from the File Type table for the site.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-44.asp In addition, this patch eliminates a side effect of the previous IIS cumulative patch (discussed in the Caveats section of Microsoft Security Bulletin MS01-026) by restoring proper functioning of UPN-style logons via FTP and W3SVC.	Internet Information Server Multiple Vulnerabilities CVE Name: CAN-2001-0506, CAN-2001-0507, CAN-2001-0508, CAN-2001-0544, CAN-2001-0545	Low/**High**	Bug discussed in newsgroups and websites. Exploit has been published for the IIS buffer overflow vulnerability. Exploit script has been published for the IIS Table Privilege Elevation vulnerability.
Microsoft[18]	Windows 2000	ISA Server 2000	Three vulnerabilities exist: a Denial of Service vulnerability exists in the Proxy service due to a memory leak; a Denial of Service vulnerability exists involving the H.323 Gatekeeper service due to a memory leak; and a cross-site scripting vulnerability exists because the ISA server fails to check the URL for the presence of script commands when generating the error page, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-045.asp This patch supersedes the one provided via Microsoft Security Bulletin MS01-021.	ISA Server Multiple Vulnerabilities CVE Name: CAN-2001-0546, CAN-2001-0547, CAN-2001-0658	Low/**High**	Bug discussed in newsgroups and websites.

[16] Bugtraq, August 20, 2001.
[17] Microsoft Security Bulletin, MS01-044, August 15, 2001.
[18] Microsoft Security Bulletin, MS01-045, August 16, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[19]	Windows 2000	Windows 2000, 2000 SP1&SP2	A Denial of Service vulnerability exists due to an unchecked buffer in the software that handles information from the IrDA (Infrared Data Association) device.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-046.asp	Windows 2000 IrDA Buffer Overflow Denial of Service CVE Name: CAN-2001-0659	Low	Bug discussed in newsgroups and websites.
Microsoft[20]	Windows NT 4.0/2000	Exchange Server 5.5, 5.5 SP1-SP4	A Denial of Service vulnerability exists in the optional component, Outlook Web Access. *Note: If this behavior is due to a buffer overrun condition, it may be possible to execute arbitrary code.*	No workaround or patch available at time of publishing.	Outlook Web Access Denial of Service	Low/**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[21]	Windows NT 4.0/2000	Windows NT 4.0 Option Pack, Windows 2000 Server SP1&SP2, Windows 2000 Advanced Server, Windows 2000 Advanced Server SP1&SP2	A remote Denial of Service vulnerability exists in the NNTP (Network News Transport Protocol) service due to a memory leak in a routine that processes news postings.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-043.asp	Windows NNTP Denial of Service CVE Name: CAN-2001-0543		Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Mirabilis[22]	Windows 95/98/ME/ NT 4.0/2000	ICQ 2001 a, 2000.0A, 2000.0b Build 3278	A vulnerability exists due to the way Internet Explorer and ICQ handle data returned from a webserver with "Content-Type: application/x-icq," which could let a malicious user force the addition of arbitrary ICQ UINs to a target user's ICQ contact list.	No workaround or patch available at time of publishing.	ICQ Forced User Addition	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[19] Microsoft Security Bulletin, MS01-046, August 21, 2001.
[20] SecurityFocus, August 22, 2001.
[21] Microsoft Security Bulletin MS01-043, August 14, 2001.
[22] Hexyn/Securax Advisory #22, August 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[23]	Windows 95/98/NT 4.0/2000, MacOS 8.1, 8.5, 8.6, 9.0, Unix	Microsoft Internet Explorer 5.0.1 SP1&SP2, 5.5; 4.0.1, 5.0, 5.0.1 for Windows 95, 98, NT 4.0, 2000; Outlook Express 4.0, 4.01, 4.27.3110.1, 4.72.2106.4, 4.72.3120.0, 4.72.3612.1700, 5.0, 5.01, 5.5; Outlook Express for MacOS 4.5, 5.0; Netscape Communi-cator 4.04-6.01; Opera Software Opera Web Browser 5.02 win32, 5.10 win32, 5.11 win32, Opera Web Browser 5.0 Linux; University of Kansas Lynx 2.7, 2.8, 2.8.4, 2.8.5	A vulnerability exists in some HTML browsers, which could let a malicious user send arbitrary data to TCP ports. This can be used to send commands to servers using ASCII-based protocols such as SMTP, NNTP, POP3, IMAP, IRC, and probably others.	No workaround or patch available at time of publishing.	Multiple Vendor HTML Form Protocol	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Multiple Vendors[24, 25]	Unix	Window-maker wmaker 0.60- 0.64	A buffer overflow vulnerability exists when X11 applications are setting the titles of their windows, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/dists/stable/updates/main/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Window Maker Window Title Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
NetCode[26]	Unix	NC Book 0.2b	A vulnerability exists in the GuestBook package, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	NC Book Book.CGI Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[23] Securiteam, August 19, 2001.
[24] Debian Security Advisor, DSA-074-1, August 12, 2001.
[25] Conectiva Linux Security Announcement, CLA-2001:411, August 13, 2001.
[26] PoizonB0x Advisory#6, pb0x-06-08-2001, August 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell[27]	Multiple	Groupwise 5.5	A vulnerability exists when indexing of directories is enabled, which could let a remote malicious user gain sensitive information.	Novell has released a GroupWise Padlock Fix, it is not yet confirmed whether or not this patch addresses this issue. However, users are encouraged to install the patch located at: http://support.novell.com/padlock/	Groupwise Directory Disclosure	Medium	Bug discussed in newsgroups and websites.
Novell[28]	Multiple	Groupwise 6.0, Groupwise Enhancement Pack 5.5	A vulnerability exists which could let a malicious user completely compromise a Groupwise system. Novell has not disclosed technical details, but the company has made a patch available.	Patch available at: http://support.novell.com/padlock	GroupWise Padlock	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
phpBB Group[29]	Unix	phpBB 1.0.0, 1.2.0, 1.2.1, 1.4.0, 1.4.1	A vulnerability exists due to improper validation of a variable in the 'bb_profile.php' script, which could let a malicious user gain access to the administrative features.	No workaround or patch available at time of publishing.	phpBB Unauthorized Administrative Features Access	**High**	Bug discussed in newsgroups and websites.
RSA Security[30]	Multiple	Keon Certificate Authority 5.7	A Denial of Service vulnerability exists in the Secure Directory Server's LDAP implementation. For more information please see Cert Advisory located at: http://www.cert.org/advisories/CA-2001-18.html	RSA has released a hotfix to its customers through its SecurCare Online service addressing this issue.	Keon Certificate Authority LDAP Denial of Service	Low	Bug discussed in newsgroups and websites.
Sage Software[31]	Windows NT 4.0/2000	MAS 200	A remote Denial of Service vulnerability exists because a malicious user can disable the server by entering the <control> x key combination ten times.	No workaround or patch available at time of publishing.	MAS 200 Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Sendmail Consortium[32]	Unix	Sendmail 8.11-8.11.5, 8.12beta10, 8.12beta12, 8.12beta16, 8.12beta5, 8.12beta7	An input validation vulnerability exists in the debugging function, which could let a malicious user compromise the full system.	Upgrade available at: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.0.Beta19.tar.gz	Sendmail Debugger Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Sixhead[33]	Unix	SIX-webboard 2.1	A vulnerability exists because ".." and "/"are not properly filtered from user input, which could let a remote malicious user gain sensitive information.	No workaround or patch available at time of publishing.	SIX-webboard 2.01 File Retrieval	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[27] Nomad Mobile Research Centre Advisory, August 14, 2001.
[28] Novell Security Advisory, August 14, 2001.
[29] SecurityFocus, August 13, 2001.
[30] SecurityFocus, August 21, 2001.
[31] Bugtraq, August 21, 2001.
[32] SecurityFocus, August 20, 2001.
[33] PoizonB0x Advisory#1, pb0x-07-07-2001, August 13, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc.[34]	Unix	Solaris 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A heap buffer overflow vulnerability exists in xlock when handling some environment variables, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	OpenView xlock Heap Overflow CVE Name: CAN-2001-0652	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Surf-Net[35]	Multiple	ASP Forum 2.20	A vulnerability exists because the ID number assigned to cookies is derived directly from the UserID, which could let a malicious user locally edit the saved cookie, substituting the appropriate administrative cookie ID number ("0888888") for the one he was assigned.	Upgrade available at: http://www.surf-net.co.uk/asp/forum/forum_script.asp	ASP Forum Predictable Cookie ID	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Symantec[36]	Windows	pcAnywhere 9.2, 10.0	A remote Denial of Service vulnerability exists when the socket on which the pcAnywhere server is listening is fed an abnormal amount of random characters immediately upon connection.	Patch available at: http://www.symantec.com/techsupp/files/pca/pca9-9598nt.html	pcAnywhere Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
TDavid[37]	Unix	TD Forum 1.2	A vulnerability exists because user-supplied HTML tags in input are not properly filtered, which could let a malicious user execute arbitrary scripts embedded in HTML.	No workaround or patch available at time of publishing.	TD Forum Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Trend Micro, Incorporated[38]	Windows NT 4.0/2000	Virus Buster Corporate Edition 3.52-3.54, OfficeScan Corporate Edition for Windows	A vulnerability exists in one of the software's web management interface programs, which could let a remote malicious user view sensitive information.	Patch available at: http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=3086	Virus Buster Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
TrollTech[39]	Unix	TrollFTPD version 1.26 and prior	A buffer overflow vulnerability exists in the way the recursive directories are handled, which could let a malicious user execute arbitrary commands and gain root privileges.	Upgrade available at: ftp://ftp.trolltech.com/freebies/ftpd/troll-ftpd-1.27.tar.gz	TrollFTPD Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Webridge[40]	Multiple	PX Application Suite	A vulnerability exists when a faulty HTTP request is sent to the server, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	PX Application Suite Internal Server Error Message	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[34] NSFOCUS Security Advisory, SA2001-05, August 10, 2001.
[35] Bugtraq, August 20, 2001.
[36] Securiteam, August 15, 2001.
[37] Bugtraq, August 20, 2001.
[38] Secure Net Service(SNS) Advisory No.38, August 20, 2001.
[39] Securiteam, August 15, 2001.
[40] Bugtraq, August 15, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
WhitSoft Development[41]	Windows 95/98/NT 4.0/2000	SlimFTPd 2.2	A directory traversal vulnerability exists because relative paths are handled incorrectly, which could let a malicious user view sensitive information.	No workaround or patch available at time of publishing.	SlimFTPd Directory Traversal	Medium	Bug discussed in newsgroups and websites.
Wind River Systems, Inc.[42]	Multiple	BSDI BSD/OS 3.0, 3.1	A Denial of Service vulnerability exists which may be due to a bad system call.	No workaround or patch available at time of publishing.	BSDI Possible Local Kernel Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Xerox[43]	Multiple	DocuPrint N40	A Denial of Service for printing services exists on hosts being scanned for potential infection of the Code Red worm.	Xerox has released a non-vulnerable firmware upgrade version 1.87-25. This firmware upgrade can be obtained by calling Xerox Support at 1-800-835-6100	DocuPrint N40 Laser Printer Code Red Denial of Service	Low	Bug discussed in newsgroups and websites.
ZyXEL[44]	Multiple	Prestige 642R-I, 642R, 202, 100	A vulnerability exists if the default password has not been changed, which could let a remote malicious user make configuration changes, perform a firmware upgrade, or change passwords.	Upgrade available at: ftp://ftp.europe.zyxel.com/public/prestige/	Prestige Router Administration Interface	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between August 10 and August 20, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security**

[41] Securiteam, August 21, 2001.
[42] Bugtraq, August 21, 2001.
[43] Bugtraq, August 10, 2001.
[44] Bugtraq, August 9, 2001.

vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 16 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	**Script name**	**Script Description**
August 20, 2001	Disengage	Tool for decrypting passwords.
August 20, 2001	**Killbsdi.c**	**Script which exploits the BSDI Possible Local Kernel Denial of Service vulnerability.**
August 20, 2001	Xp.tar.gz	Script which exploits the Sendmail Debugger Arbitrary Code Execution vulnerability.
August 19, 2001	Top.c	Script that exploits the FreeBSD 3.3 x86 top format string vulnerability.
August 18, 2001	Airsnort-0.0.9.tar.gz	Tool for wireless LANs that recovers encryption keys by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. This works on both 40-bit and 128-bit encryption.
August 18, 2001	Exp_w3m.pl	Perl script that exploits the FreeBSD w3m remote buffer overflow vulnerability.
August 17, 2001	Gl123dos.pl	Perl script which exploits the glFtpD LIST Denial of Service vulnerability.
August 15, 2001	Achilles-0-27.zip	A tool for Windows designed for testing the security of web applications. Achilles is a proxy server which acts as a man-in-the-middle during an HTTP session. It will intercept an HTTP session's data in either direction and give the user the ability to alter the data before transmission.
August 15, 2001	Gps-0.6.0.tar.gz	Ghost Port Scan is an advanced port scanner and a firewall rule disclosure tool that uses IP & ARP spoofing, sniffing, and stealth scanning to allow penetration testers and system administrators to test the settings of a remote host.
August 15, 2001	Iiscrack.zip	Script which exploits the IIS Table Privilege Elevation vulnerability.
August 15, 2001	**Phrack57.tar.gz**	**In this issue: IA64 shellcode, Ethernet Spoofing with Taranis, ICMP based OS Fingerprinting, Vudo Malloc Tricks, Once upon a free(), Against the System: Rise of the Robots, Holistic approaches to attack detection, NIDS on Mass Parallel Processing Architecture, Modern SSL Man-in-the-middle attacks, Architecture Spanning Shellcode, Writing ia32 Alphanumeric Shellcode, Cupass and the Net user change password problem.**
August 15, 2001	Taranis-0.81.tar.gz	Taranis redirects traffic on switch hardware by sending spoofed Ethernet traffic.
August 15, 2001	Trock.c	Script which exploits the TrollFTPD Buffer Overflow vulnerability.
August 14, 2001	Store.cgi.txt	Exploit URL for the Store.cgi vulnerability.
August 10, 2001	**Sol_sparc_xlockex.c**	**Script which exploits the OpenView xlock Heap Overflow vulnerability.**
August 10, 2001	**Sol_x86_xlockex.c**	**Script which exploits the OpenView xlock Heap Overflow vulnerability.**

Trends

Probes/Scans:

There has been an increase in scans of port 23 probing for the Multiple Vendor TelnetD vulnerability. (For more information, see the Multiple Vendor Telnetd Buffer Overflow

vulnerability described in CyberNotes 2001-15 [July 30, 2001] located at http://www.nipc.gov/cybernotes/2001/cyberissue2001-15.pdf.)

CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.

Other:

The National Infrastructure Protection Center (NIPC) continues to work in close coordination with its public and private sector partners regarding what has been named Code Red II. The NIPC considers Code Red II to be a serious threat because it spreads rapidly and installs a backdoor that can be accessed by anyone familiar with the exploit. For more information, see : NIPC ADVISORY 01-017 located at: http://www.nipc.gov/warnings/advisories/2001/01-017.htm.

Microsoft has developed a tool that eliminates the obvious damage that is caused by the Code Red II worm. For more information, see "Tool to Remove Obvious Effects of the Code Red II Worm" available at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/redfix.asp.

Internet backbone providers have notified the NIPC they are witnessing large-scale victimized web servers scanning for Microsoft Internet Information Server (IIS) vulnerabilities. The activity of the Code Red worm has the potential to degrade services running on the Internet. Any web server running the Microsoft IIS versions 4.0 or 5.0 that is not patched is susceptible to infection and exploitation as an attack platform. The NIPC is strongly urging consumers running these versions of IIS 4.0/5.0 to check their systems and install the patch. For more information, see NIPC ADVISORY 01-015, located at: http://www.nipc.gov/warnings/advisories/2001/01-015.htm or NIPC ALERT 01-016, located at http://www.nipc.gov/warnings/alerts/2001/01-016.htm. The Microsoft bulletin describing this vulnerability and its patch to fix the problem may be found at: http://www.microsoft.com/technet/security/bulletin/MS01-033.asp (also in CyberNotes-2001-13).

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Magistr	File, Worm	Slight Increase	March 2001
2	W32/SirCam	Worm	Slight Decrease	July 2001
3	VBS/Loveletter	Script	Increase	March 2000
4	W32/Hybris	Worm	Slight Decrease	November 2000
5	PE_MTX.A	File Infector, Trojan	Stable	September 2000
6	W32/Funlove	File	Slight Increase	November 1999
7	VBS/Stages	Script	Slight Increase	June 2000
8	VBS/SST (Anna K)	Script, Worm	Return to Table	February 2001
9	VBS/Kakworm	Script	Stable	December 1999
10	W32/BadTrans	Worm	Decrease	April 2001

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **208** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **487** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

Eumel.383 (Alias: Eumel.363.A) (DOS Virus): This is a DOS virus that infects only .com files that are in the same folder as the virus.

VBS.IO.A@mm (Alias: VBS.Thea.A) (Visual Basic Script Worm): This worm sends an e-mail message to all contacts in the victim's Microsoft Outlook address book. The message contains a link to the virus writer's home page. The worm also modifies mIRC settings on the infected computer.

VBS.Peace.Worm (Visual Basic Script Worm): This is a simple worm that attempts to copy itself to drive F.

VBS.Proud.A@mm (Visual Basic Script Worm): This is a worm that creates hundreds of files that have the file extensions .doc, .xls, .ppt, and .jpg. It then opens a Web page related to soccer and sends e-mail to all contacts in the Microsoft Outlook address book.

VBS_UPDATE.A (Aliases: UPDATE.A, VBS_LODING.A, VBS/Loding@MM, VBS/Loding, VBS_UPDATE, Computer Secrets, Loding): (Visual Basic Script Worm): Upon execution, this Visual Basic Script (VBS) worm sends e-mails to all addresses listed in a host computer's address list. It does not have any other destructive payload.

VBS.XPMsg@mm (Visual Basic Script Worm): This is a simple Visual Basic Script (VBS) worm that sends e-mail to all contacts in the victim's Microsoft Outlook address book. It searches for all files that have extensions that begin with .ht; for example, .html, .hta, and .htm. It then copies itself to those files.

W32.Invictus.dll (Win32 Virus): Invictus.dll is a dynamic link library (.dll) file that can be used by viruses for replication purposes. On its own it does nothing. Invictus.dll exports the following functions:

- TempPath
- _close_file
- _infect_file
- _open_create
- _open_read
- _open_write

NOTE: The Invictus.dll file imports code from the Windows file Imagehlp.dll. If Imagehlp.dll is not installed on the system, Invictus.dll will not function. When an infected file (that uses the Invictus.dll file) is opened, two things will happen:

1) The Invictus.dll file is copied to the \System folder.
2) The virus itself is copied to the Windows \Temp folder and executed from there.

W32/Jerrym (Alias: Worm.JerryMsg.A) (Win32 Worm): This is a worm that spreads via MSN Messenger using the filename PIC1324.EXE. On execution it creates the registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSN Messenger

which it points to the executable. It also creates a folder called C:\Messenger1234\Brain. The worm then places into this folder a file called 1ReadMe.txt, which contains removal instructions.

W32/Petik-K (Alias: Troj/Petik-K) (Win32 Worm): This is an e-mail-aware worm which attempts to facilitate its proliferation by pretending to be connected to the popular French TV show “Loft Story.” The worm copies itself to the Windows directory as loft_story.exe and to the Windows System directory as loft.exe. It changes WIN.INI so that loft.exe will run automatically each time Windows is started. It then displays a message box with the title “Loft Story” and the body text “I’m fucking the Loft Story” before quitting. When run from the Windows System directory, the worm creates the following Registry key:

HKCU\Software\Microsoft\PetiK

It drops loft.htm into the Windows Startup directory and waits for an Internet connection. When the worm detects an Internet connection, it displays a message box with the title “Loft Story” and the text “Welcome to Internet!”. It will then search for e-mail addresses in *.htm* files in the Internet file cache subdirectory and attempt to send itself to those addresses as an e-mail attachment. The e-mail has the following characteristics:

Subject: “Loft Story News...”
Message body: “The last video of the program”
Attached file: loft_story.exe

On the 28th of any month the worm will set the following registry keys:

HKCU\Software\Microsoft\Internet Explorer\Main\Start Page = “http://www.loftstory.fr”
HKLM\Software\Microsoft\Windows\CurrentVersion\RegisteredOrganization= “LoftStory”
HKLM\Software\Microsoft\Windows\CurrentVersion\RegisteredOwner = “Aziz, Kenza, Loanna, etc.”

Next it displays the message, “New Worm Internet coded by PetiK (c)2001.” The HTML file dropped by W32/Petik-K contains a VBScript that modifies the following registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ActiveX 1.0 = “C: \ActiveX.vbs”
HKCU\Software\Microsoft\Internet Explorer\Download Directory = “C:\”

It will also change the Registry entry for the Internet Explorer start page, setting it to download a VBScript file from http://www.ctw.net.

W32.Zoek@mm (Aliases: I-Worm.Zoek.b, I-Worm.Zoek.dll) (Win32 Worm): This worm arrives as an e-mail message that contains a link to an executable named Results.exe which is hosted on a Web site. When activated, this worm creates the following files on the infected system:

C:\Windows\System\Tcasutaw.exe - (the backdoor component)
C:\Windows\Accountboy.ini
C:\Windows\Installboy.ini
C:\Windows\Mailboy.ini
C:\Windows\Tcasuta.exe - (the mailer)
C:\Windows\Tcasutav.dll - (part of the mailer)

It then activates the backdoor component, which creates the registry value

tcasutaw.exe C:\Windows\System\tcasutaw.exe

in the following key

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

Finally, it sends a copy of the e-mail message to all contacts in the Windows address book.

WM97/Hope-AD (Word 97 Macro Virus): This is a corrupted variant of the WM97/Hope-A Word macro virus. The corruption has been caused by interaction with another macro virus.

WM97/Marker-GP (Word 97 Macro Virus): This virus has been reported in the wild. This is a corrupted but viable variant of WM97/Marker-C. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers hacking site and appends this information to the bottom of the macro as comments.

WM97/Marker-JG (Word 97 Macro Virus): This is a Word macro virus. Whenever a document is closed on the first day of any month, this member of the WM97/Marker virus family attempts to FTP user information from Word to a website belonging to the Codebreakers hacking group. It also appends this information to the bottom of the macro as comments.

XM97/Laroux-OE (Excel 97 Macro Virus): This is an Excel spreadsheet virus. This variant of the XM97/Laroux family creates the viral file Negs.xls in the XLSTART directory. The virus has no malicious payload.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow:	**N/A**	**Current Issue**
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Penrox	**N/A**	**Current Issue**
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
BAT.Install.Trojan	N/A	CyberNotes-2001-04
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07

Trojan	Version	CyberNotes Issue #
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
CodeRed II	II	CyberNotes-2001-16
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
HardLock.618	N/A	CyberNotes-2001-04
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.StartPage	N/A	CyberNotes-2001-07
JS_OFFENSIVE.A	**N/A**	**Current Issue**
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	**N/A**	**Current Issue**
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
StealVXS	**N/A**	**Current Issue**
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	**N/A**	**Current Issue**
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DSNX.A	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAI.A	**N/A**	**Current Issue**
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICMPBOMB.A	**N/A**	**Current Issue**
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_KEYLOG.25	**N/A**	**Current Issue**
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	**N/A**	**Current Issue**
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_NEWPIC.A	**N/A**	**Current Issue**
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	**N/A**	**Current Issue**
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01

Trojan	Version	CyberNotes Issue #
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	**N/A**	**Current Issue**
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.Offensive	**N/A**	**Current Issue**
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan.Xtratank	**N/A**	**Current Issue**
Trojan.Zeraf	**N/A**	**Current Issue**
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS.Zync.A	**N/A**	**Current Issue**
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
Y3K Rat	1.6	CyberNotes-2001-11

Adshow: This program alters the default start page of Internet Explorer for the purpose of displaying advertisements. As this program is configurable, specific details surrounding infection may vary. When run, the Trojan installs itself on the local system by copying itself to C:\WINDOWS\ADSHOW.EXE and creating a WIN.INI RUN value to load itself at startup:

```
RUN=ADSHOW.EXE
```

An HTML page (configured to display remote HTML pages with advertisements) is saved to the file HOMEPAGE.HTM, and BACS.DAT in the WINDOWS SYSTEM directory and the following registry key value are set to configure Internet Explorer to use this page as the default start page:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\ Main\Start Page=c:\windows\system\homepage.htm

The file HM.DAT is created in the WINDOWS directory. This file contains the default start page of Internet Explorer prior to the infection (or whichever page is configured after the infection). The ADSHOW.EXE program hooks IE such that when a user attempts to look at the configured default start page with the Internet Options menu, the actual value is concealed and URL specified in HM.DAT is displayed instead. Additionally, the file GBV.EXE may be written to the DESKTOP. This is an installer for the Greeting Browser Viewer, which requires user intervention for it to be installed.

Backdoor.Penrox: This is a backdoor Trojan that allows unauthorized access to a compromised computer. When Backdoor.Penrox is run, it first queries the operating system to determine what its file name is. This file name is then used by the Trojan when it makes the following change to the Windows registry:

It adds the value

TaskReg <path and file name of Backdoor.Penrox>

to the following key

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that it runs every time that Windows starts. Next, Backdoor.Penrox sends the malicious user who controls the Trojan information about the infected computer by connecting to an IRC channel that is monitored by the hacker. Thereafter, the compromised system also listens for commands from the hacker.

JS_OFFENSIVE.A (Aliases: FLUG, FLUG.A, JS@Juck, Trojan.Offensive, JS/Offensive, Offensive): Upon execution, this Trojan modifies the registry so that the infected system is unable to execute any applications. The modifications also remove certain links from the Start Menu, leaving only Windows Update, Programs, and Help links. The infected computer can no longer execute any applications such as the MS-DOS prompt. This Trojan disables the infected user's access to drives installed on the system when the "My Computer" folder is opened. It also disables the "Shut Down Windows" function so that pressing the Reset button is the only way to restart the computer. The modifications in the registry entries also hide the desktop icons upon system restart.

QDel172 (Aliases: BAT_NIEMALS.A, VBS.AutoExec.Trojan, VBS_NIEMALS.A): This is a VBScript Trojan contained in an HTML document. When the document is accessed and the script is allowed to run, it overwrites the C:\AUTOEXEC.BAT file to contain instructions to delete all files in the C:\, C:\WINDOWS, and C:\WINDOWS\SYSTEM directories. The HTML page contains the following text:

Was meinst du ist ist sicherheit?
Dein PC?
Nichts ist sicherheit!
Alles was real ist auf dieser erde ist nicht sicher!
Niemals
Never be the secure!
(c) _ **-** [DaS_cHaoS] **-**

StealVXS: This Trojan is dropped by a program that contains a utility for generating decryption codes for digital/satellite key cards. When the program is run, it drops the Trojan into a file called SYSTRAY.DLL in the WINDOWS SYSTEM folder and then runs invisibly. The utility is also dropped into a file called TEMPO.EXE in the WINDOWS TEMP folder where it is then executed. The Trojan creates the following registry key to load itself at startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\ RunServices "SysTray.dll"

Next the Trojan searches the current drive for a file called VXS.KEY. If the file is not found, then the Trojan exits. However, if the file is found, then the Trojan e-mails the file using the computer's current SMTP e-mail account to an Internet mailbox, after which it exits.

TROJ_ALLGRO.A (Aliases: W32.ALLGRO.A@mm, I-worm.Atirus): This Internet worm propagates via e-mail using the default mail client. The e-mail it sends has the subject line "New antivirus tool" and the body contains the text “Hey, checkout this new antivirus tool which checks your system for viruses.” The e-mail arrives with the attachment ANTIVIRUS.EXE. This Trojan was created using Borland C++.

TROJ_DSNX.A (Aliases: DSNX, DSNX.A, Trojan.Win32.DSNX): This destructive Win32 Trojan enables a remote malicious user to access an infected computer, compromising network security. Upon execution, this Trojan copies itself to a file named WIN<text>.EXE in the Windows System directory, where <text> is a randomly generated text string. It then adds the following registry entry that allows it to run at every boot up:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run = WinDSNX

The Trojan then connects to an IRC server and joins a channel where the remote malicious user is connected; the remote user may execute any of the following actions on an infected system:

Upload/Download files
Perform a port scan on the local area network
Flood a specified IP address
Log keystrokes
Delete files

TROJ_HAI.A (Aliases: HAI, HAI.A, W32.Hai.worm): Upon execution, this network Trojan/worm searches for potential victims that have fully shared the \Windows directory; if one is found, it copies itself to this directory. It also adds an entry to the run field in the WIN.INI file. It has no destructive payload.

TROJ_ICMPBOMB.A (Alias: ICMPBOMB.A): This Trojan program causes a Denial of Service (DoS) attack. It is an “ICMP Bomber” tool that a malicious user uses to crash a target computer. It sends ICMP packets in increasing size to a system. Upon execution, it displays a graphical user interface where the user inputs the IP address of a target computer, the size of the data to be sent to the target computer, and the time interval between each data burst. This Trojan contains the following text strings:

“ICMP Bomber!”

TROJ_KEYLOG.25 (Aliases: KEYLOG, KEYLOG.25): This KeyLogger Trojan records every key stroke on a computer where it is active, and it saves all these keystrokes in a file located in the C:\Windows\Temp folder. It has no destructive payload.

TROJ_MODNAR.A (Aliases: TROJ_MODNAR, W32/Modnar@MM, W32.Modnar.Worm@mm, TROJ_DOCPIF.A, DOCPIF, DOCPIF.A): This Win32 Trojan propagates via e-mail using the default mail client. It randomly generates the subject, message body, and attachment of the e-mails it sends out using letters of the alphabet. However, the subject and message body always end with both a punctuation mark and a question mark (e.g., “!?”). This worm was coded in Visual C/C++. Some of its variants are UPX compressed. It has no destructive payload.

TROJ_NEWPIC.A (Aliases: TROJ_BRAIN.A, BRAIN, BRAIN.A, TROJ_NEWPIC.A): This program is written in Visual Basic 6. It is a Trojan/worm that propagates via MSN messenger by sending copies of itself to users in an infected user’s contact list. It creates a folder and drops the file 1README.TXT. This worm appears in the Task Manager as the process “MsgSprd.” Once the Trojan is installed on the infected system and is active in memory, it will attempt to spread by sending a copy of itself to other systems chatting with the infected PC via MSN Messenger. The first time a connection is established between the infected PC and a non-infected system, the Trojan will send this message:

“hey, want me to send my new pic?” “I took it yesterday”

It sends this together with the real message being sent by the user of the infected system. The Trojan then waits for the target system’s message. If the message contains any of the words:

“send”
“yes”
“yea”
“ok”
“guess”
“maybe”
“sure”

it will send a copy of itself to the target system with the response “there” for send;, “alright, here ya go” for yes, yea, and ok; “I hope you like it” for guess; and “pweese ? :-) for maybe. There is no response for “sure.” The Trojan file is sent to a target system only once. The Trojan creates a marker file at C:\messenger1324\brain to check whether a connection was already established before.

TROJ_OPTIX.SVR (Aliases: OPTIX, OPTIX.SVR, TROJ_OPTIX.CLI, Backdoor.Optix.01): This server-side hacking tool enables a remote malicious user to upload and execute files on an infected user’s computer. Upon execution, this server-side Trojan copies itself into the Windows directory and modifies the registry to run at every boot up. The registry entry, the filename, and the port number for this Trojan may vary. It then opens a port that listens for commands from a remote user running the client program. Some anti-virus tools detect the client side that controls this server-side hacking tool as TROJ_OPTIX.CLI. When the client program is executed, it displays a graphical user interface where a remote hacker enters the IP address of the computer infected with the server component in order to establish a connection. Thereafter, the client component can upload files, including other malware, to the infected computer. It is also capable of executing these uploaded programs on the remote system. The client side also has a built-in server editor that allows the hacker to change the Filename, Port number, Password, Registry name, and behavior of the server program.

Trojan.JS.Clid.gen: This is a generic detection entry for a Trojan horse that comes in the form of an .html file, most often sent to potential victims by e-mail. These Trojans exploit ActiveX capabilities which give them full control over a compromised computer. Most of these Trojans modify the Web browser’s home page and restrict access to the system in some minor way, typically by blocking access to the browser’s Internet settings. Microsoft has released a patch which will close the security vulnerability exploited by these Trojans. Users can download the patch from the following Microsoft site: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/ms00-081.asp.

Trojan.Offensive: This is a Trojan horse that comes in the form of an .html file. (It could also be a Web page on the Internet). When opened, the page displays one button that contains the text “Start.” This Trojan exploits ActiveX capabilities, which allows it to modify the browser’s home page, as well as to severely restrict the victim’s access to his system. If the Trojan has been activated, victims should either contact a computer professional for assistance or consider reinstalling Windows.

Trojan.Xtratank: This is a simple Trojan horse that causes the computer to stop responding.

Trojan.Zeraf: This is a destructive Trojan horse that deletes critical system files. If it has been executed, Windows will no longer be able to run. It is programmed in Delphi and distributed as a UPX-packed, self-extracting RAR archive. (UPX is a runtime compressor for Windows executable files). When the Trojan is run, it inserts the Trojan executable on the hard disk as C:\Zeraful\Zeraful.exe and then executes that file.

VBS.Zync.A (Alias: VBS.Snights): VBS.Zync.A is a small Visual Basic Script (VBS) threat. On the 13th of any month this Trojan changes the registered owner and organization names to those of the virus writer. On the 6th and 11th of the month, there is a 1-in-4 chance that it will format drive C.